




# Managing Security Vulnerabilities in Your Commercial-off-the-Shelf (COTS) Systems Using an Industry Standards Effort

Robert A. Martin  
The MITRE Corporation

**24 October 2002**

# Outline

-  **Background and Motivation**
  - 0 Finding Out About Vulnerabilities**
  - 0 The Problem and a Solution - CVE**
  - 0 CVE Compatibility**
  - 0 The CVE Process**
  - 0 Summary**

# DoD's Move to IP will Leverage Commercially Available Capabilities... and Liabilities....

## POLICY

## STRATEGIES

### Air Force wires weapons to Web

Plan pushes more info to warfighters

BY GEORGE I. SEFFERS

**T**he U.S. Air Force is requiring that all command and control systems and weapon systems be wired to the World Wide Web.

John Gilligan, an Air Force deputy chief information officer, said that the Web-enablement policy offers several benefits, including universal access to data, a reduction in personnel and lower costs.

"The intent is really to establish a formal way that we will Web-enable, we will use XML [Extensible Markup Language], and we will use [Internet Protocol]," Gilligan said. By using IP to connect the data links, he said the Air Force will be able to use commercially available capabilities.

Air Force Secretary James Roche and Gen. Michael Ryan, outgoing Air Force chief of staff, signed the policy July 9.

Web-enabling technologies and standards to govern information interchange and promote greater interoperability," the document states.

The memo calls specifically for the use of four technologies: IP, XML, URLs and Web browsers.

Currently, most weapon and command and control systems use a plethora of protocols and are not always able to share data. That means the data has to be manually transferred from one system to another, and sometimes it cannot even be accessed or found. XML is a "far superior data exchange protocol," Gilligan said.

"The first benefit would be the ability

to find information. We have found that just by providing a link to systems, it opens up information universally," Gilligan said.

Lt. Gen. John Woodward, the other Air Force deputy CIO and the service's director of communications and information, estimates that operational power is the biggest benefit from data exchange. The



"N  
HAW  
BUT  
A VI  
Jo

**Woodward acknowledged that weapon systems wired to the Web will be even more vulnerable to information warfare attacks and said that information will have to be assured and additional vulnerabilities will simply have "to be dealt with."**

# Many Motivations for Getting on top of Vulnerabilities

<http://www.cert.org/advisories/CA-2002-06.html>

**CERT® Advisory CA-2002-06 Vulnerabilities in Various Implementations of the RADIUS Protocol**

Original release date: March 4, 2002  
Last release: —  
Source: CERT/CC

A complete revision history can be found at the end of this file.

**Systems Affected**

Systems running any of the following RADIUS implementations:

- Ascend RADIUS versions 1.18 and prior
- Citron RADIUS versions 1.8.5 and prior
- FreeRADIUS versions 0.3 and prior
- GnuRADIUS versions 0.35 and prior
- ICRADIUS versions 0.18.1 and prior
- Livingston RADIUS versions 2.1 and earlier
- RADIUS (previously known as Lucent RADIUS) versions 2.1 and prior
- RADIUS versions 0.3.1 and prior
- xTRADIUS 1.1 and prior

<http://www.theregister.co.uk/content/53/24244.html>

**The Register**

in association with The Register and salmondays.tv proudly presents

**Salmon Days**

A digital streaming sysadmins blockbuster

**Staying on top of Oracle's holes**

By **Thomas C. Greene** in Washington

Posted: 28/02/2002 at 12:28 GMT

In light of the fortnight-old SNMP pandemic, it's tempting to forget that the world's most popular database kit remains vulnerable to a host of

## Security quandary: Who's liable?

By Dennis Fisher and Chris Gonsalves in San Jose, Calif.

**S**KITTEN AT THE PROSPECT OF BEING held liable for security breaches, software vendors are examining ways to get ahead of problems with solutions ranging from restrictive user agreements to forced security patches.

The movement is in response to a growing sense that lawsuits will be the next

tool used to counter expensive security problems such as the Code Red and Nimda worms, according to industry insiders.



Musdie: Automate.

"Whose responsibility is the long tail of infections that goes on after the initial explosion of activity with something like Nimda?" asked Dan Geer, chief technology officer at @Stake Inc., a security consulting company based in Cambridge, Mass.

@Stake last week released a report showing that 70 percent of the security defects found in an analysis of its customers' networks were the result of software design flaws. "Applications are our current biggest security risk. Automatic security updates [could be] made part of the license agreement as a way to address that," Geer said.

To that end, Microsoft Corp., of Redmond, Wash., is looking for a way to automatically distribute patches to enterprise customers, much the same way home

(continued on Page 14)



**INSIDE:** 15 COMPAQ USERS WARY OF HP TAKEOVER // 19 NEWS.GOV: BUSH ADMINISTRATION WANTS AN FOIA EXEMPTION // 20 MICROSOFT EXEC DISCUSSES .NET // 25 UNPLUGGED: UWB TECHNOLOGY CAUSING CONCERN // 29 ROUTESCIENCE CUTS TRANSACTION TIME

FEBRUARY 25, 2002 11 @WEEK

JODY C. PATILLA: THE HOT LINE

## SECURITY: TIME TO TAKE NAMES, LAY BLAME

THERE WERE TWO INTERESTING DEVELOPMENTS LAST MONTH in the realm of information security. One was the release of a new report by the National Academy of Sciences; the other was the apparent Saul-on-the-road-to-Tarsus conversion of the NAS report, "Cybersecurity Today and Tomorrow: Pay Later," observes that

often neglected because it is. But the most attention-grabbing recommendation is for policy-makers to consider "legislative retooling" making vendors

responsible for security breaches. The recommendation is going to change in the way we

handle such legislation will work. Assessment of liability depends on shared assumptions about what constitutes adequate security efforts and on whom the burden of making those efforts rests. Currently, the security burden lies with the consumer to keep up with patches, but that has become an overwhelming task. Since it is less costly and less disruptive to write secure software up front than it is to clean up from

hundreds of systems later, the bulk of the burden should lie with the vendor. Unfortunately, under current law, software vendors apparently have little motivation to assume that burden. Consider the buffer overflow. We've known about it since the dawn of programming. Therefore, it's reasonable to state that vendors that release software containing buffer overflows are guilty out of sloppy programming but also of willfully disregarding security. Grounds for a lawsuit, then? Maybe, but only if

you can show that you sustained some level of damage. Still, imagine the consequences if hundreds of angry corporate customers joined in a class action suit over, say, bug-diddled Web server software. I'm astonished this hasn't happened yet.

**CURRENTLY, THE SECURITY BURDEN LIES WITH THE CONSUMER, BUT THAT HAS BECOME OVERWHELMING.**

the talk, starting by changing development practices and accountability. I've said it here before, and I'll say it again: Bill, security has to be baked in, not painted on. Get cooking. #

Maybe such a nightmare helped propel Bill Gates into sending his security memos. Now Microsoft will have to walk

Jody C. Patilla, a security consultant, can be reached at jcp@musdieconsulting.com.

<http://www.baselinemag.com/article/0,3658,s=1867&a=23195,00.asp>

<http://www.eweek.com/article/0,3658,s=701&a=23193,00.asp>

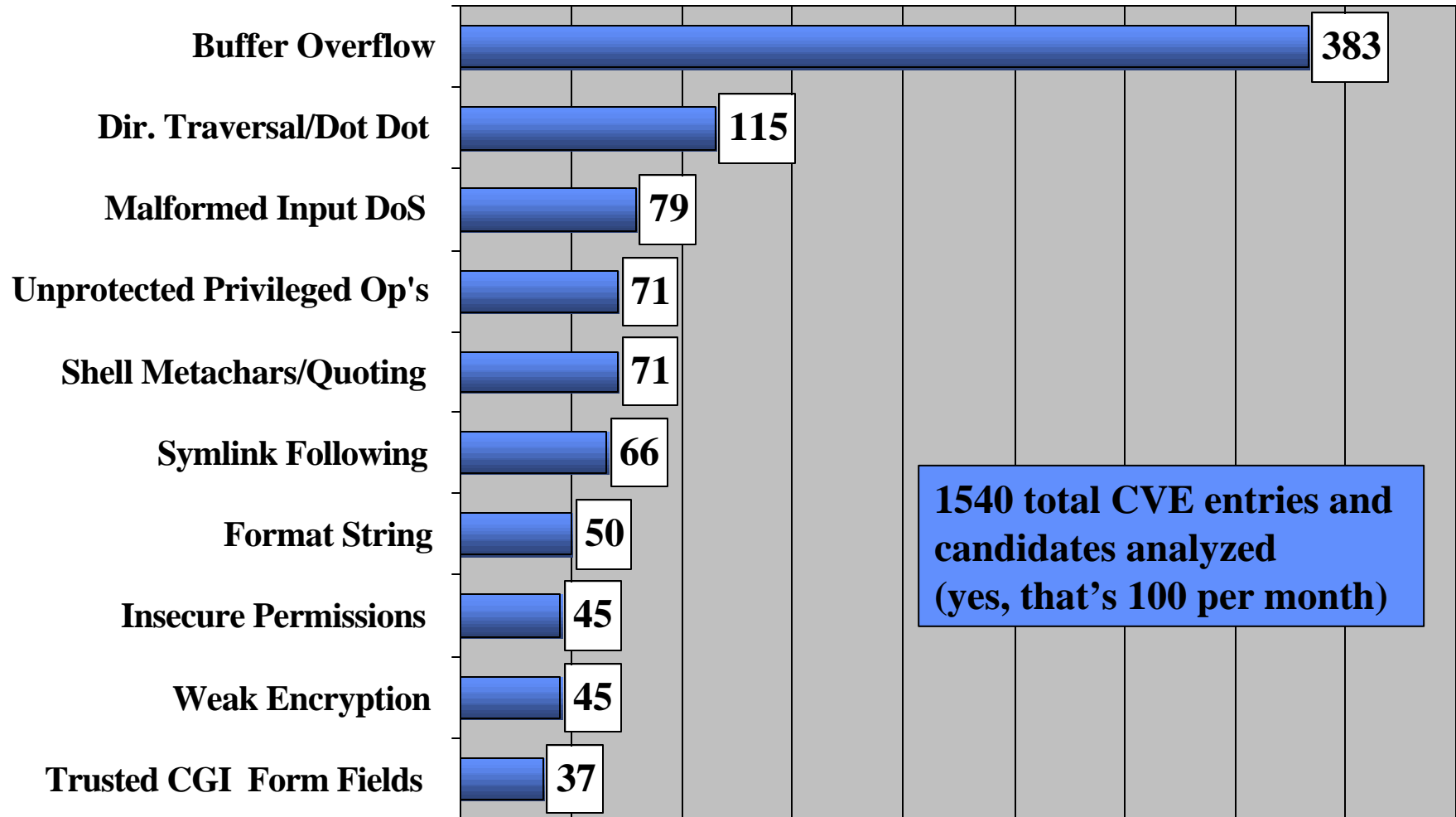


# Software problems with security implications are referred to as Vulnerabilities or Exposures

- 0 **Vulnerabilities** are security related software problems that could directly allow serious damage
- 0 **Examples:**
  - phf, ToolTalk, Smurf, rpc.cmsd, etc.
  - Oracle XSQL servlet 1.0.3.0 and earlier allows remote attackers to execute arbitrary Java code by redirecting the XSQL server to another source via the xml-stylesheet parameter in the xslt stylesheet. *[9 Jan 01 Georgi Guninski]*
- 0 **Exposures** are security related software problems that could be used as stepping stones for a successful attack
- 0 **Examples:**
  - Running finger, poor logging practices, etc.

# Top Ten Vulnerability Types in CVE



(Issues publicized between Jan 2000 and April 2001)



# Vulnerabilities Have Been Found in Almost Every Type of Commercial Software There Is



## Mail Servers

1st Up Mail Server  
All-Mail  
ALMail32  
Avirt Mail Server  
Becky! Internet Mail  
CWMail  
Domino Mail Server  
Exchange Server  
Hotmail  
Internet Anywhere Mail Server  
ITHouse Mail Server  
Microsoft Exchange  
Pegasus Mail  
Sendmail


## Security Software

ACE/Server  
BlackICE Agent  
BlackICE Defender  
Certificate Server  
CProxy Server  
ETrust Intrusion Detection  
GateKeeper  
InterScan VirusWall  
Kerberos 5  
Norton AntiVirus  
PGP  
SiteMinder  
Tripwire

## Web servers & tools

Domino HTTP Server  
IIS  
NCSA Web Server  
Sawmill  
WebTrends Log Analyzer



## Internet

AFS  
Apache  
BIND  
CGI  
Cron  
IMAP




## Routers

3220-H DSL Router  
650-ST ISDN Router  
Ascend Routers  
Cisco Routers  
R-series routers




## Network Applications

BackOffice  
Meeting Maker  
NetMeeting






## DBMSs

Access  
DB2 Universal Database  
FileMaker Pro  
MSQL  
Oracle




## Desktop Applications

Acrobat  
Clip Art  
Excel  
FrameMaker  
Internet Explorer  
Napster client  
Notes Client  
Novell client  
Office  
Outlook  
PowerPoint  
Project  
Quake  
R5 Client  
StarOffice  
Timbuktu Pro  
Word  
Works  
Workshop




## Development Tools

ClearCase  
ColdFusion  
Flash  
Frontpage  
GNU Emacs  
JRun  
WebLogic Server  
Visual Basic  
Visual Studio




## Operating Systems

AIX  
BeOS  
BSD/OS  
DG/UX  
FreeBSD  
HP-UX  
IRIX  
Linux  
MacOS Runtime for Java  
MPE/iX  
NetWare  
OpenBSD  
Palm OS  
Red Hat  
Security-Enhanced Linux  
Solaris  
SunOS  
Ultrix  
Windows 2000  
Windows 95  
Windows 98  
Windows ME  
Windows NT






## Firewalls

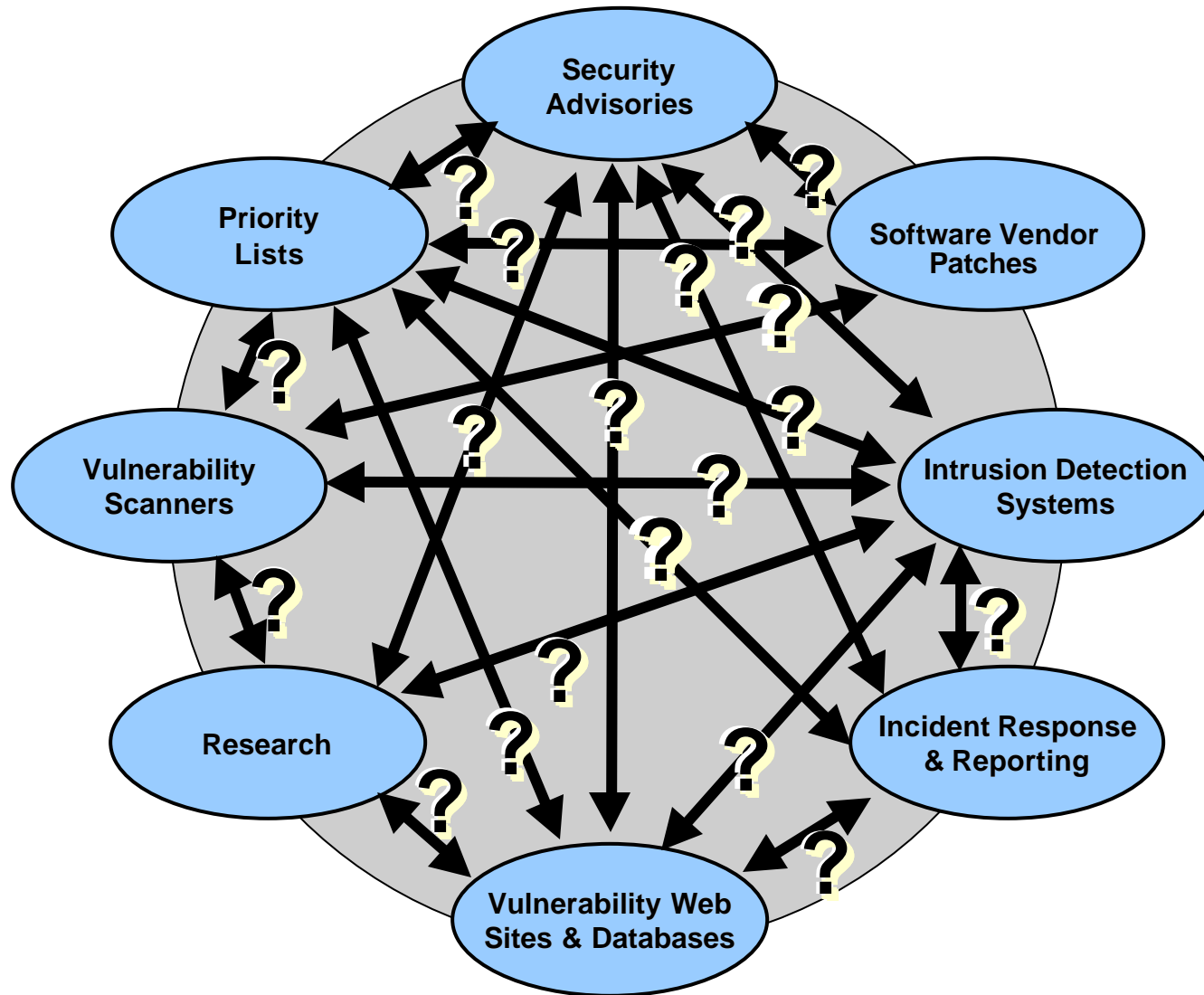
Firewall-1  
Gauntlet Firewall  
PIX Firewall  
Raptor Firewall  
SOHO Firewall



# Outline


- 0 Background and Motivation
-  Finding Out About Vulnerabilities
  - 0 The Problem and a Solution - CVE
  - 0 CVE Compatibility
  - 0 The CVE Process
  - 0 Summary

# Difficult to Integrate Information on Vulnerabilities and Exposures





# Outline

- 0 Background and Motivation
- 0 Finding Out About Vulnerabilities
-  The Problem and a Solution - CVE
- 0 CVE Compatibility
- 0 The CVE Process
- 0 Summary

# The adoption of CVE Names by the Security Community is starting to address this problem

## Organization

CERT

CyberSafe

ISS

AXENT

Bugtraq

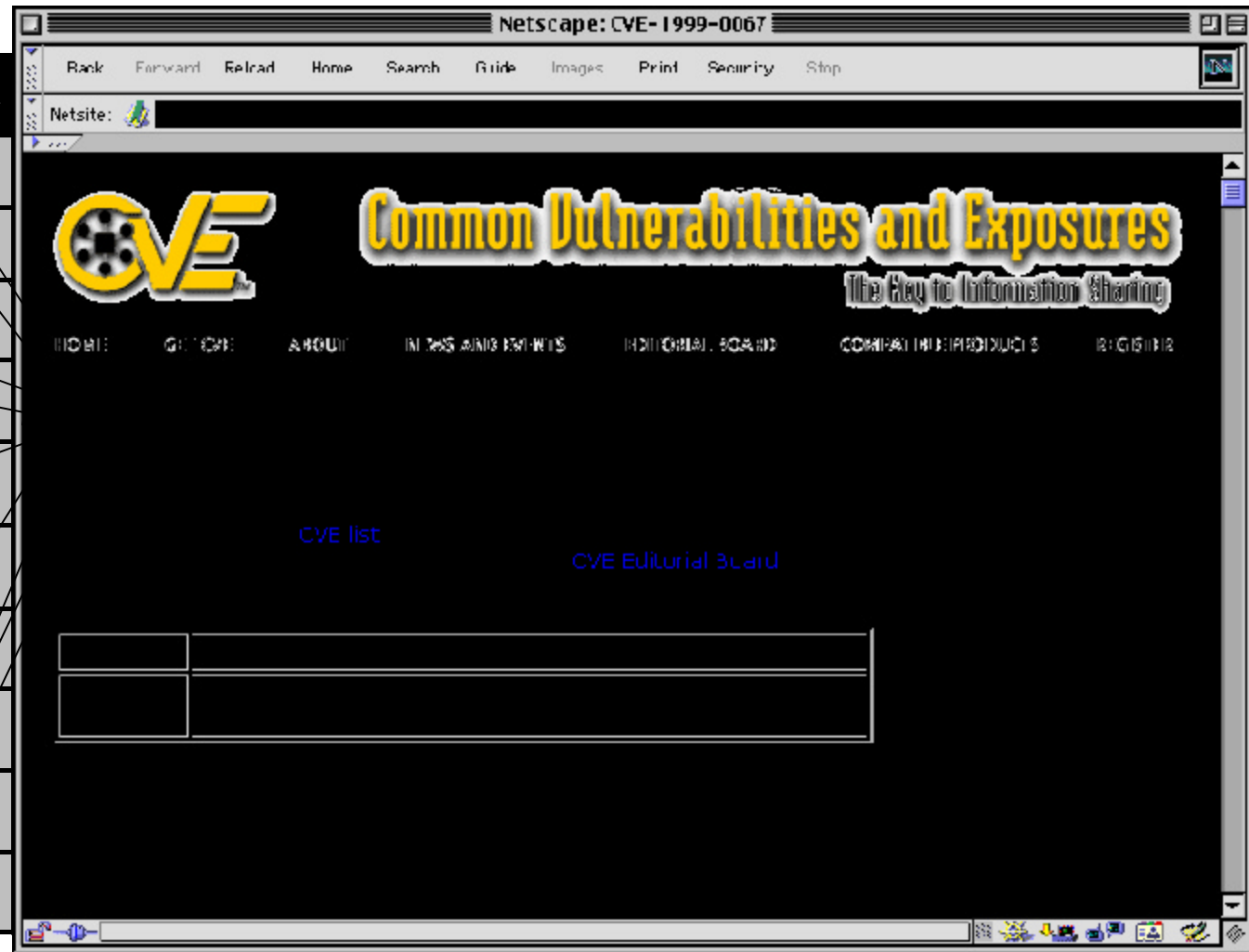
BindView

Cisco

IBM ERS

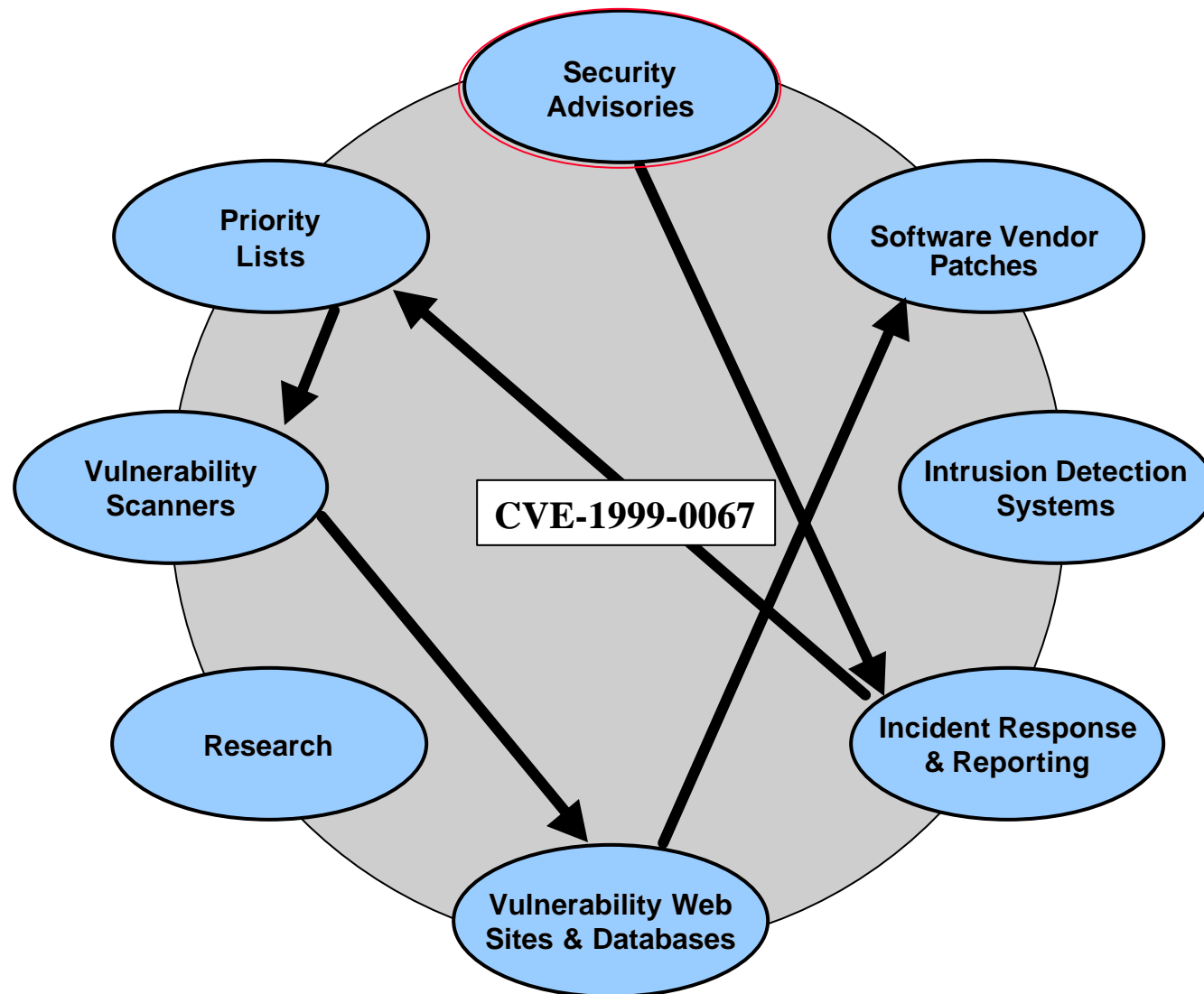
CERIAS

NAI



*Along with the new rule, “Whoever finds it, gets a CVE name for it”*

# The CVE List provides a path for integrating information on Vulnerabilities and Exposures

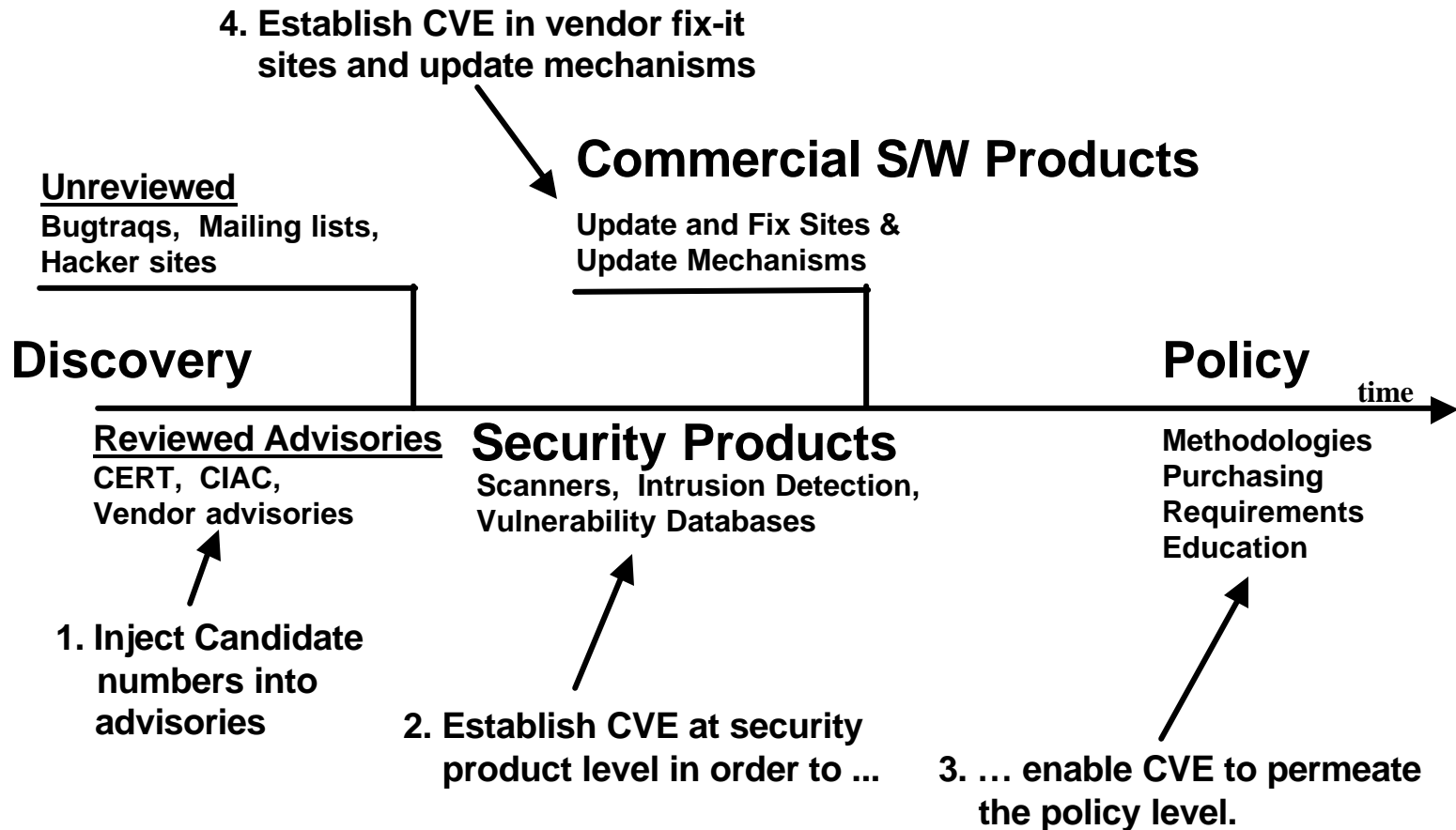


# The Common Vulnerabilities and Exposures (CVE) Initiative

- 0 An international security community activity led by MITRE focused on developing a list that provides common names for publicly known information security vulnerabilities and exposures.
- 0 Key tenets
  - One name for one vulnerability or exposure
  - One standardized description for each vulnerability or exposure
  - Existence as a dictionary rather than a database
  - Publicly accessible for review or download from the Internet
  - Industry participation in open forum (editorial board)
- 0 The CVE list and information about the CVE effort are available on the CVE web site at [cve.mitre.org]

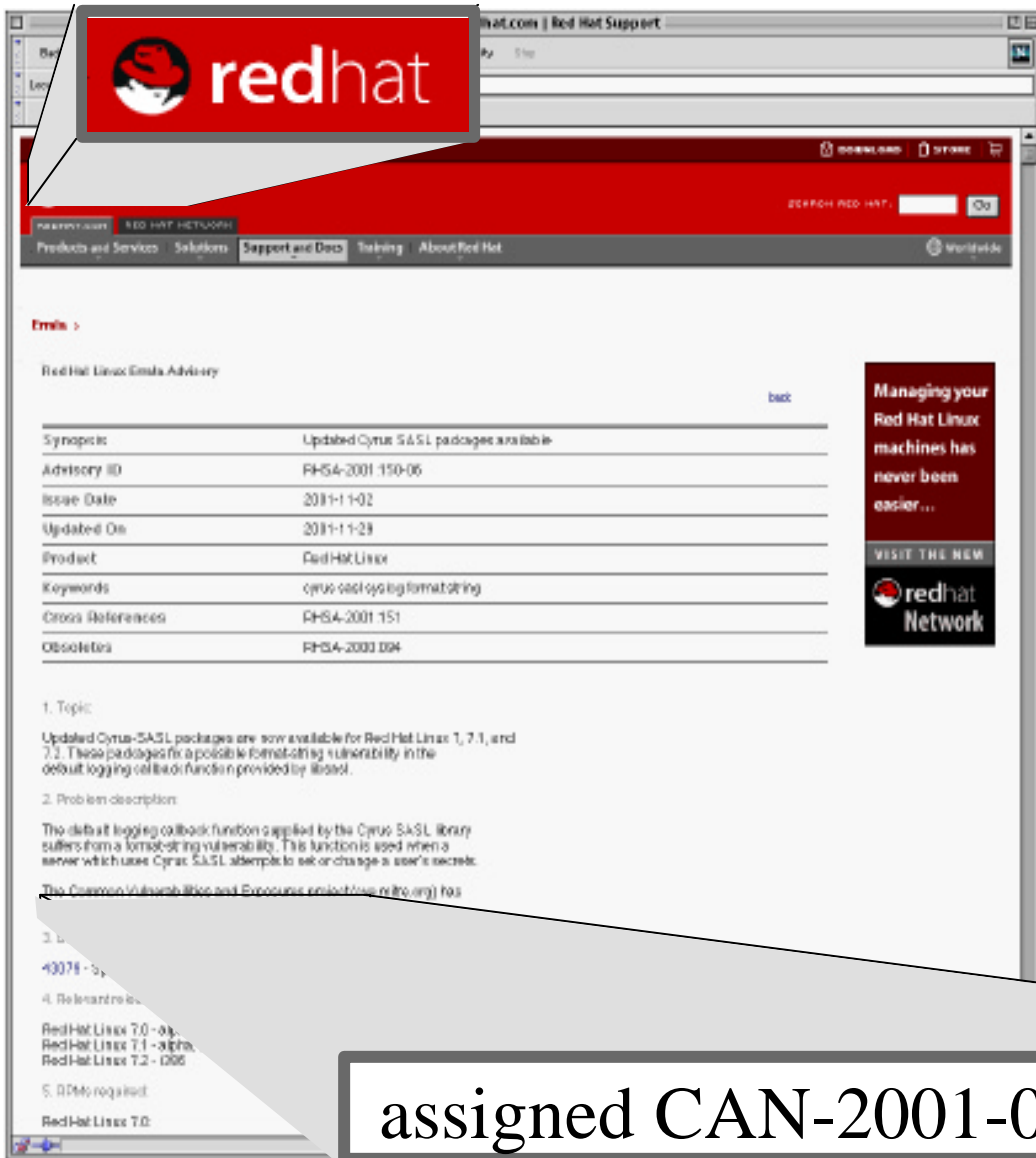


# The CVE Strategy





# Many organizations are reserving CVE names and using them in their alerts and advisories



**redhat**

Managing your Red Hat Linux machines has never been easier...

Errata >

Red Hat Linux Errata Advisory

back

Synopsis	Updated Cyrus SASL packages available
Advisory ID	RHSA-2001-150-06
Issue Date	2001-11-02
Updated On	2001-11-09
Product	Red Hat Linux
Keywords	cyrus-sasl, cyrus-sasl, formatting
Cross References	RHSA-2001-151
Obsoletes	RHSA-2001-094

1. Topic

Updated Cyrus-SASL packages are now available for Red Hat Linux 7.0, 7.1, and 7.2. These packages fix a possible format-string vulnerability in the default logging callback function provided by libssl.

2. Problem description

The default logging callback function supplied by the Cyrus SASL library suffers from a format-string vulnerability. This function is used when a server which uses Cyrus SASL attempts to ask or change a user's secrets.

The Common Vulnerability and Exposure project (cve.org) has

3. CVE ID

43076 - 5

4. Relevant releases

Red Hat Linux 7.0 - alpha  
Red Hat Linux 7.1 - alpha  
Red Hat Linux 7.2 - 0206

5. DPMs required

Red Hat Linux 7.0


To-date, CVE names have been included in initial advisories from:

- ISS X-Force
- Rain Forest Puppy
- BindView
- CERT/CC
- COMPAQ
- Ernst & Young
- CISCO
- NSFOCUS
- SecurityFocus
- VIGILANTe
- Apple
- IBM
- @stake
- HP
- SGI
- Microsoft
- eEye
- Rapid 7
- Sanctum
- Red Hat
- Apache

<http://www.redhat.com/support/errata/RHSA-2001-150.html>

assigned CAN-2001-0869 to this issue.

# Outline

- 0 Background and Motivation
- 0 Finding Out About Vulnerabilities
- 0 The Problem and a Solution - CVE
-  CVE Compatibility
- 0 The CVE Process
- 0 Summary

# What does CVE-compatible mean?

- 0 **CVE-compatible means that a tool or database can “speak CVE” and correlate data with other CVE-compatible products**
- 0 **CVE-compatible means it meets the following requirements:**
  - **Can find items by CVE name (CVE searchable)**
  - **Includes CVE name in output for each item (CVE output)**
  - **Provided MITRE with “vulnerability” item mappings to validate the accuracy of the product or services CVE entries**
  - **Makes a good faith effort to keep mappings accurate**

# Organizations With Products That Use CVE

(as of 15 October 2002)

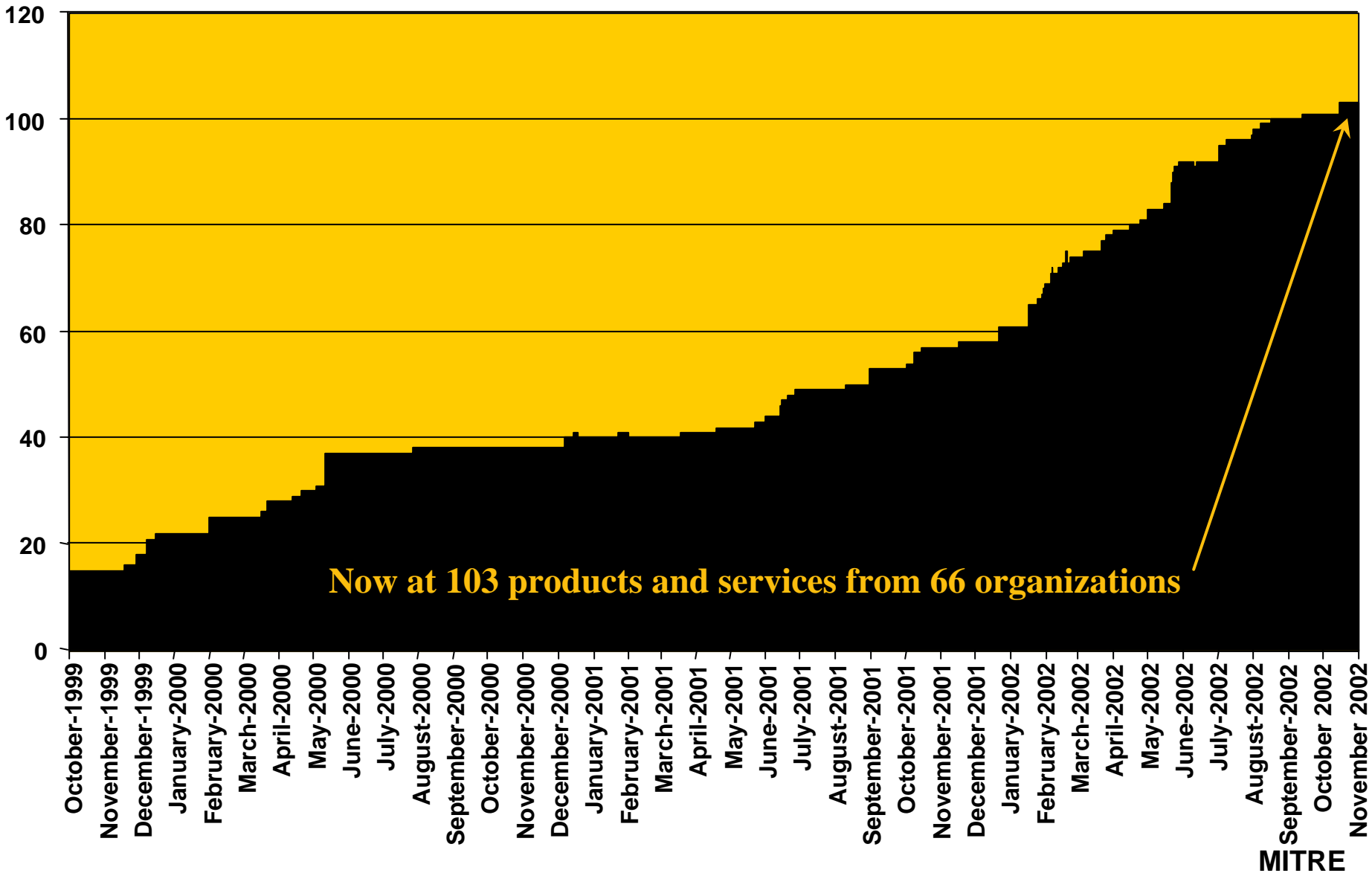
## 0 These (66) organizations have publicly declared that they are working on (103) CVE-compatible tools, databases, web sites, or services

Advanced Research Corp	NetSecure Technology, Inc.
Alliance Qualité Logiciel	Network Associates Inc.
Application Security, Inc.	Network Security Systems
Archer Technologies LLC	NIST
ArcSight, Inc.	NFR Security
BindView Corporation	NSFOCUS Information Technology Co., Ltd
CERIAS/Purdue University	N-Stalker, Inc.
CERT Coordination Center	nSecure Software (P) LTD.
Cert-IST	OneSecure
Cisco Systems	Penta Security Systems
Citadel Security Software, Inc.	Qualys
CSS ( <i>China National Computer Software &amp; Technology Service Corporation</i> )	Rapid 7 Inc.
E*MAZE Networks S.P.A	Red Hat Inc.
E-Soft Inc.	SAINT Corporation ( <i>formerly World Wide Digital Security, Inc.</i> )
eEye Digital Security	Sanctum Inc.
Enterasys Networks ( <i>bought Network Security Wizards</i> )	SANS
Entercept Security Technologies	SecureInfo Corporation
esCERT-UPC	SecureSoft, Inc.
eSecurityOnline	Security Focus, Inc.
Foundstone, Inc.	SecurityWatch
FuJian RongJi Software Development Company, Ltd	Shake Communications Pty Ltd
Harris Corporation	Snort.org
Internet Security Systems	spiDYNAMICS
Intranode	Strongbox Security Inc. (SSI)
INTRINsec	Symantec Corporation
IntruVert Networks Inc.	Tiger Testing
Inzen	Tivoli Systems Inc.
Kavado Inc.	Tsinghua UnisNet Technology, Ltd.
Kingnet Security Inc.	UC Davis, Computer Security Lab
LURHQ Corporation	Venus Information Technology Inc.
nCircle ( <i>formerly Hiverworld</i> )	VIGILANTE ( <i>merged with Cyrano's Networks Vigilance subsidiary</i> )
The Nessus Project	Vigilix, Inc.
NetIQ	Wins Technet Co., Ltd.

Up-to-date list at <http://cve.mitre.org/compatible>

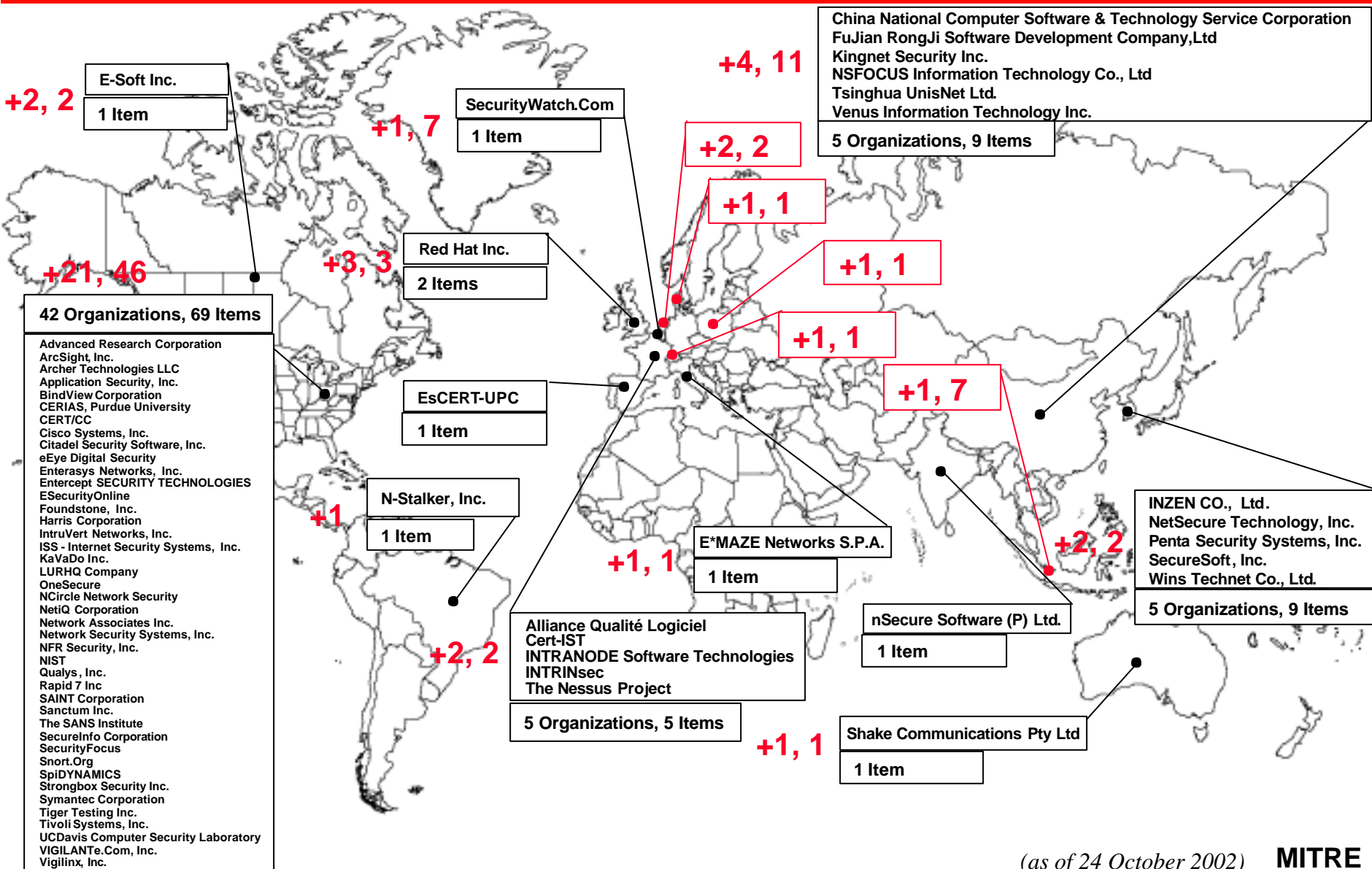
# Timeline of CVE Compatibility Declarations

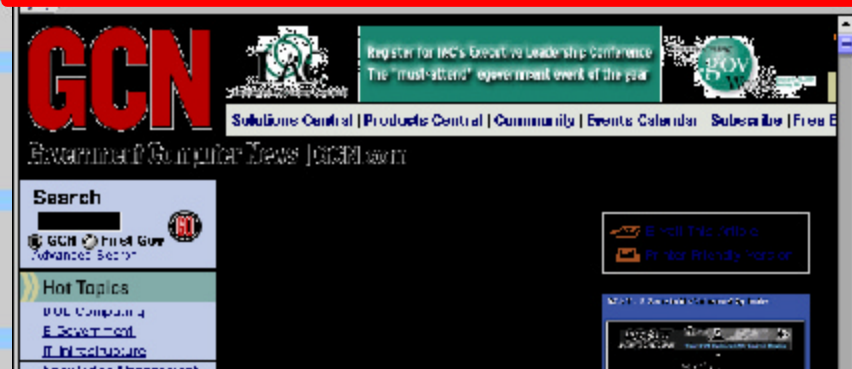
(as of 15 October 2002)





# Where CVE-compatible Items Have Come From and Where the New Ones Are Coming From






## CVE-names

***<http://icat.nist.gov>***

# Examples continued: Cassandra



**Incident Response Database**

**CERIAS**  
Center for Education and Research in Information Assurance and Security

**New User**

An email will be sent with a "challenge" password; it will not be possible to log in without the password. The objective of this is to validate your email address and limit unauthorized access.

User login:

Initial password:

Repeat password:

email address:

passwords must be at least 8 characters long **Required field**

**Cassandra (based on NIST's ICAT)**

Profile 'mheroux' for user mheroux

Products	Keywords	Searches
<input checked="" type="checkbox"/> Keep? Application <input checked="" type="checkbox"/> AntiSniff <input checked="" type="checkbox"/> AntiVirus <input checked="" type="checkbox"/> ARP protocol <input checked="" type="checkbox"/> BIND <input checked="" type="checkbox"/> Browser <input checked="" type="checkbox"/> BSDOS <input checked="" type="checkbox"/> Cable modem <input checked="" type="checkbox"/> Eudora <input checked="" type="checkbox"/> Fingerd <input checked="" type="checkbox"/> FireWall-1 <input checked="" type="checkbox"/> FTP <input checked="" type="checkbox"/> Ftpd <input checked="" type="checkbox"/> Glibc <input checked="" type="checkbox"/> Gnome-Lokkit <input checked="" type="checkbox"/> HTTP	No keywords yet Examples: <input type="text" value="'setuid', 'macro'"/> <input type="button" value="Add"/>	<a href="#">All entries</a> <a href="#">1 year</a> <a href="#">6 months</a> <a href="#">3 months</a> <a href="#">this month</a> <a href="#">Incremental</a> <a href="#">[Shows new]</a>

**ARP protocol**

[CAN-1999-0667](#) The ARP protocol allows any host to spoof ARP replies and poison the ARP cache to conduct IP address spoofing or a denial of service.

**BIND**

[CVE-1999-0009](#) Inverse query buffer overflow in BIND 4.9 and BIND 8 Releases.

[CVE-1999-0010](#) Denial of Service vulnerability in BIND 8 Releases via maliciously formatted DNS messages.

[CVE-1999-0011](#) Denial of Service vulnerabilities in BIND 4.9 and BIND 8 Releases via CNAME record and zone transfer.

[CVE-1999-0024](#) DNS cache poisoning via BIND, by predictable query IDs.

[CVE-1999-0184](#) When compiled with the -DALLOW\_UPDATES option, bind allows dynamic updates to the DNS server, allowing for malicious modification of DNS records.

[CVE-1999-0833](#) Buffer overflow in BIND 8.2 via NXT records.

[CVE-1999-0837](#) Denial of service in BIND by improperly closing TCP sessions via so\_linger.

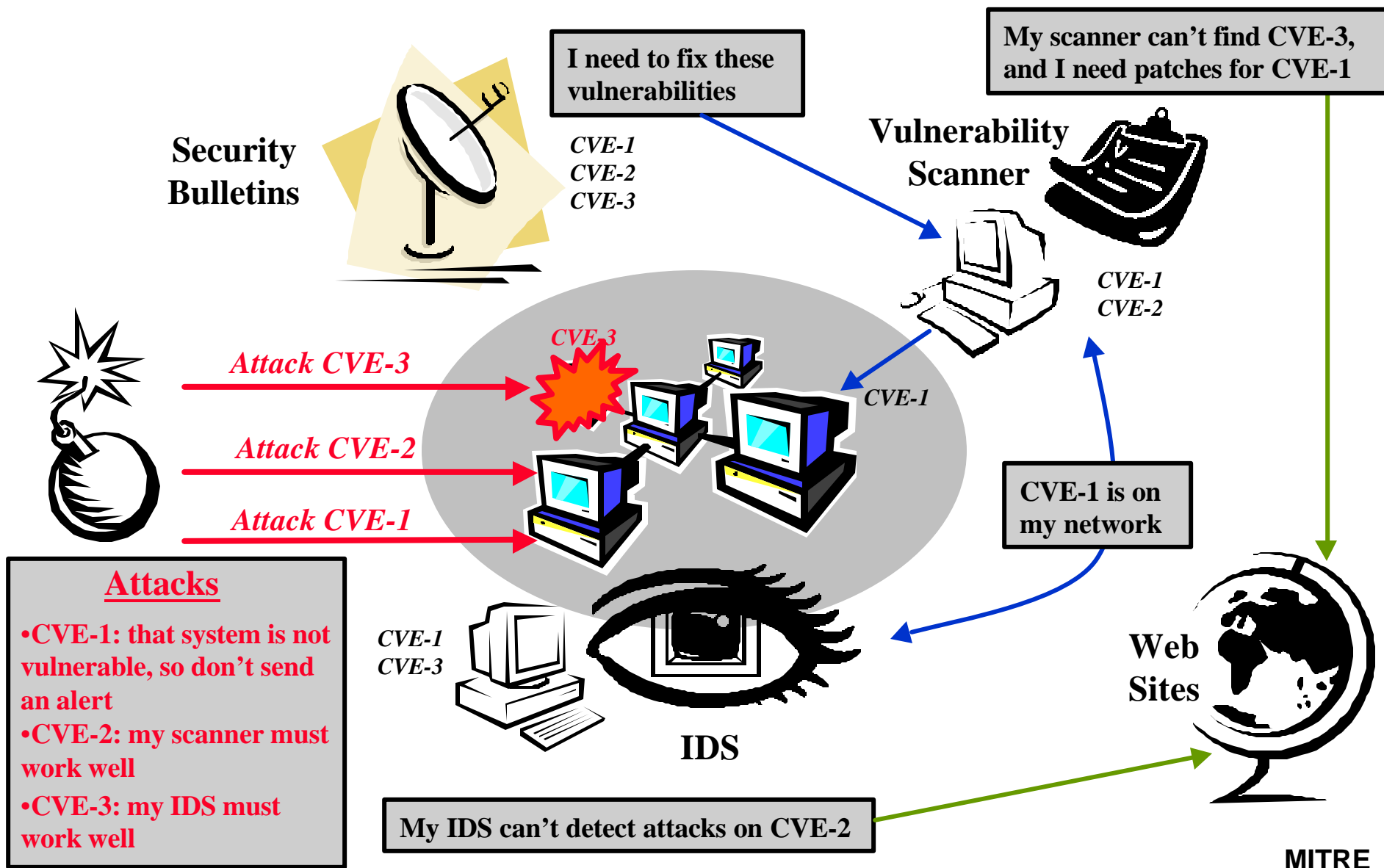
[CVE-1999-0848](#) Denial of service in BIND named via consuming more than fdmax file descriptors.

[CVE-1999-0849](#) Denial of service in BIND named via maxname.


[CVE-2000-0335](#) The resolver in glibc 2.1.3 uses predictable IDs, which allows a local attacker to spoof DNS query results.

**CVE-names**

# Using CVE in the Enterprise



# Outline

- 0 **Background and Motivation**
- 0 **Finding Out About Vulnerabilities**
- 0 **The Problem and a Solution - CVE**
- 0 **CVE Compatibility**
-  **The CVE Process**
- 0 **Summary**



## ***Council Roles***

- 0 Act as a catalyst for CVE and related activities.**
- 0 Assure funding for the core CVE activity over the long term including outreach to Government organizations and agencies.**
- 0 Discuss community needs and possible new CVE services.**
- 0 Promote the adoption of CVE at the strategic level.**
- 0 Business planning & prioritization.**
- 0 Discuss CVE and related security policy implications for the Federal Government.**
- 0 Identify CVE related materials & resources for use by Government CIOs and senior managers.**



# CVE Senior Advisory Council Members

## Co-Chairs:

- 0 John Gilligan, CIO of the USAF, and Co-chair of the Architecture/Interoperability Committee of the CIO Council
- 0 Sallie McDonald, GSA Assistant Commissioner Office of Info Assurance and Critical Infrastructure Protection



## Participating Organizations

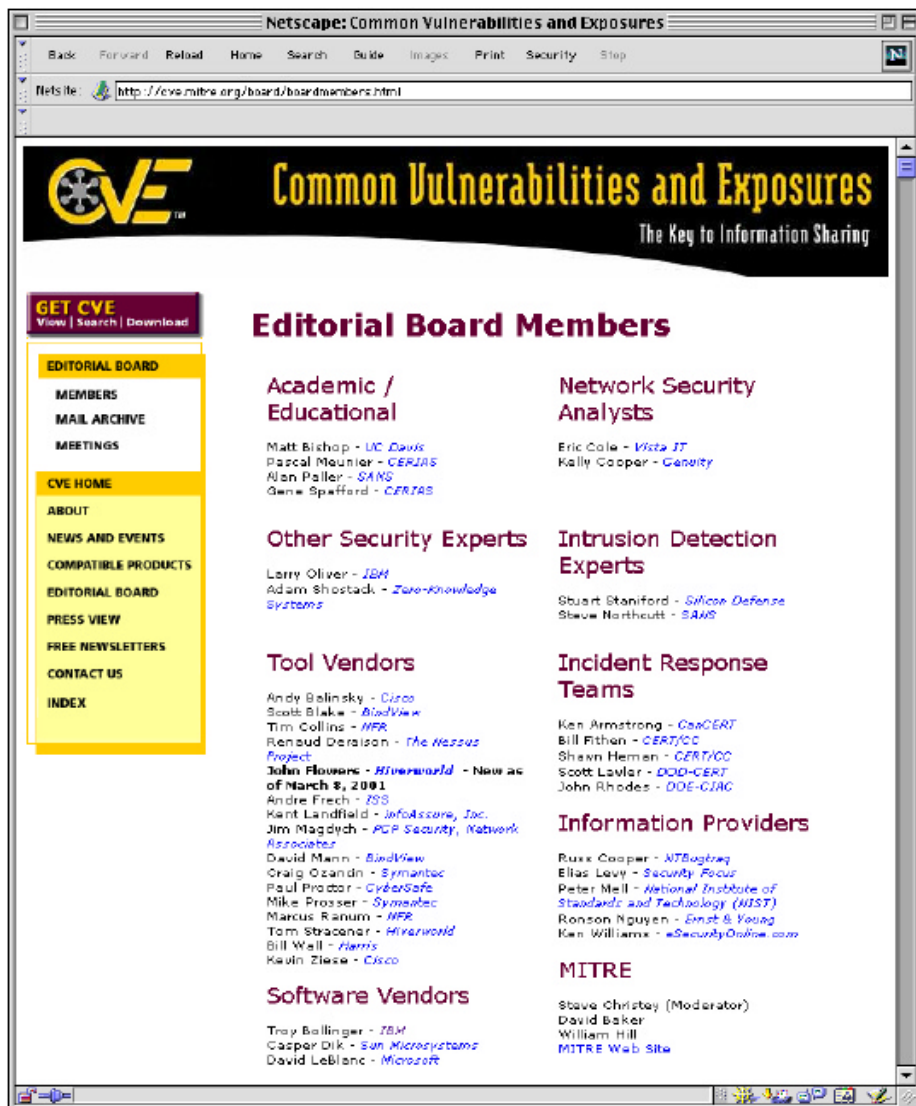
- 0 Department of the Treasury
- 0 Department of Energy
- 0 Department of Labor
- 0 Department of Health and Human Services
- 0 Internal Revenue Service
- 0 National Institute of Standards and Technology
- 0 Critical Infrastructure Assurance Office
- 0 National Infrastructure Protection Center
- 0 Office of Management and Budget

- GSA
- DISA
- NSA
- NASA
- ASD/C3I
- Air Force
- Intelligence Community



# CVE Editorial Board

- 0 Includes mostly technical representatives from 30 different organizations including researchers, tool vendors, response teams, and end users
- 0 Reviews and approves CVE entries
- 0 Discusses issues related to CVE maintenance
- 0 Holds monthly meetings (face-to-face or phone)
- 0 Maintains publicly viewable mailing list archives  
[[cve.mitre.org/board/archives](http://cve.mitre.org/board/archives)]



# CVE Editorial Board



eSecurity Online



Genuity



infoAssure



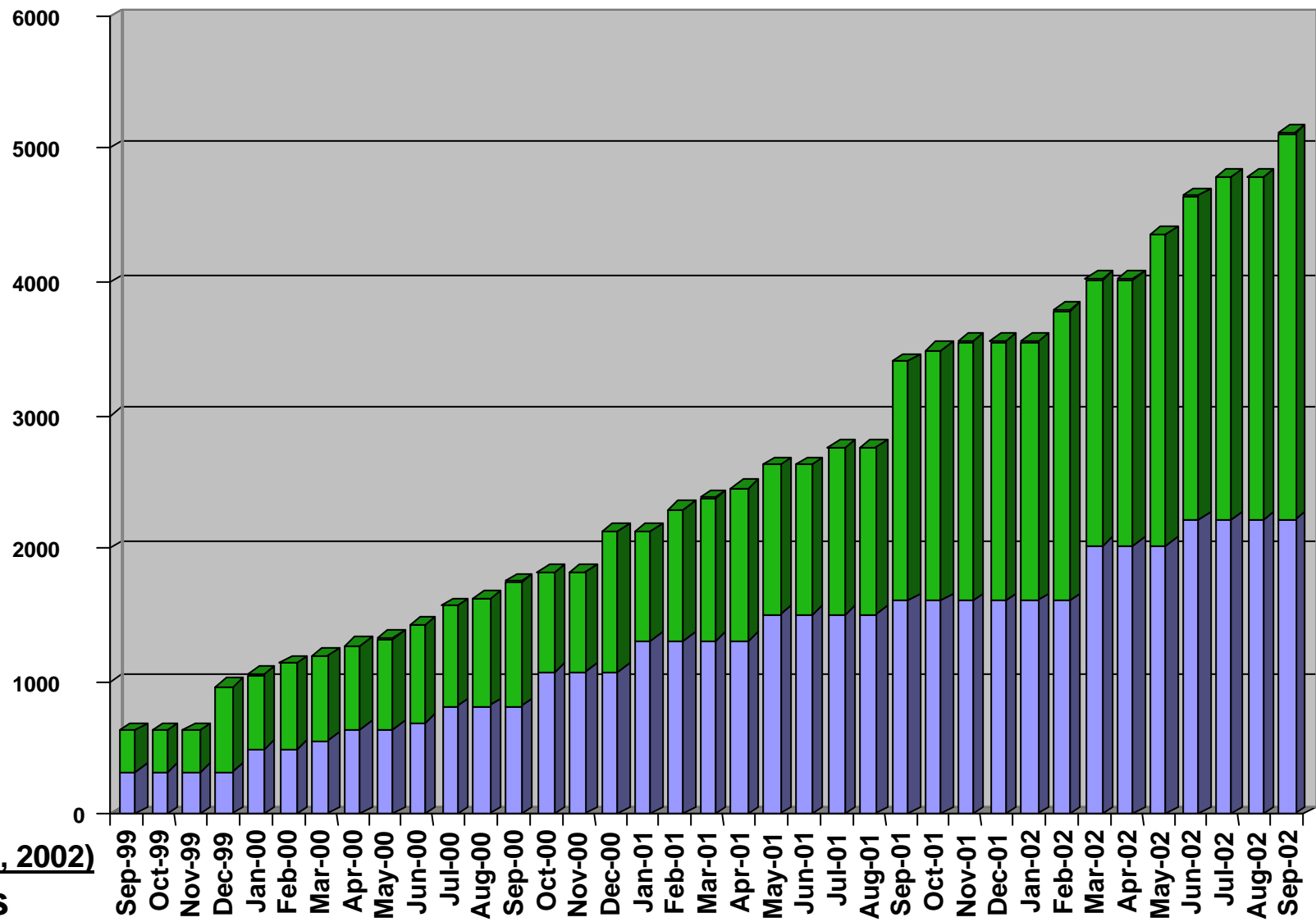
zeroknowledge

Sun Microsystems



MITRE

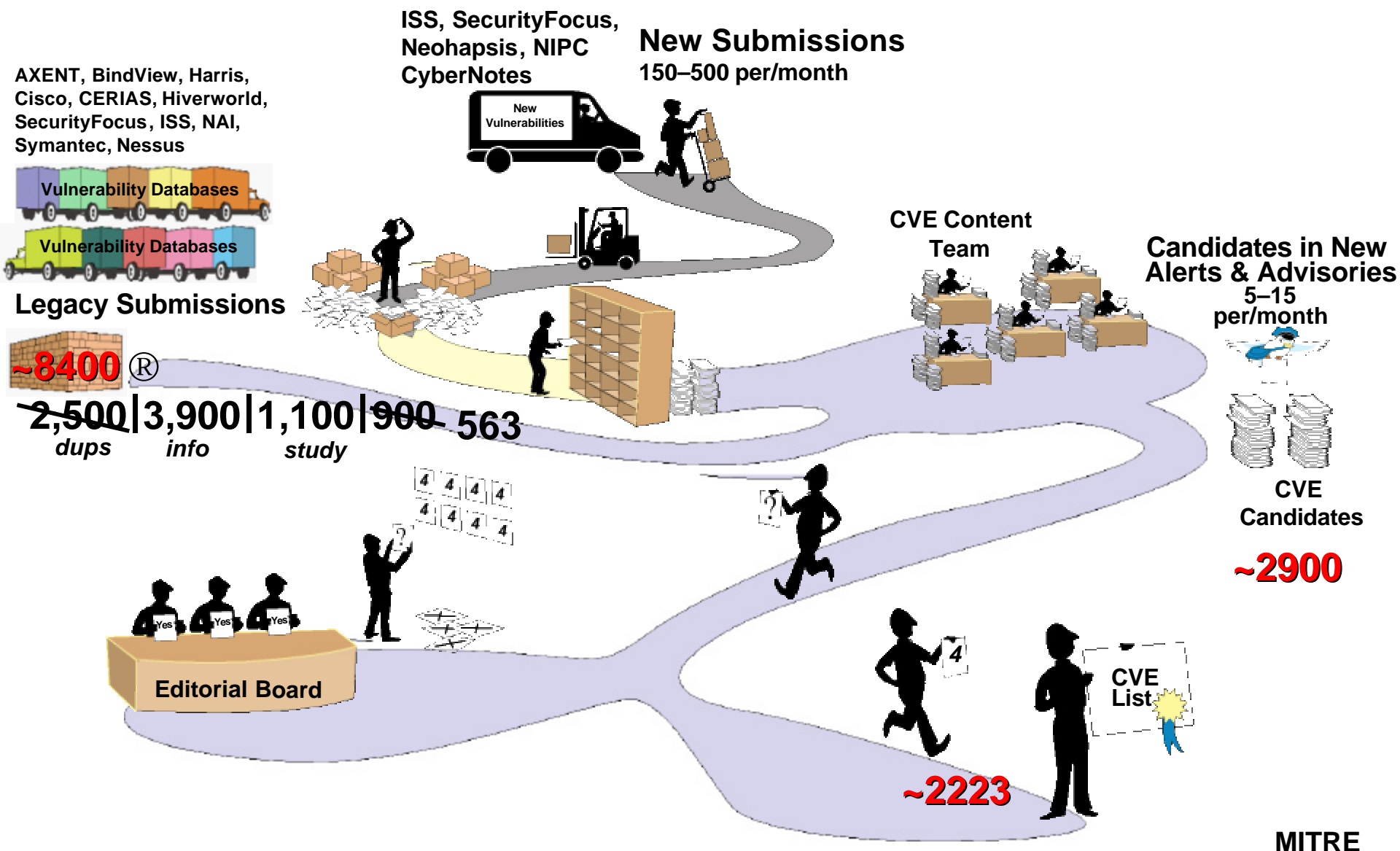
# CVE Growth



**Status**  
(as of August 30, 2002)


- 2223 entries
- 2900 candidates

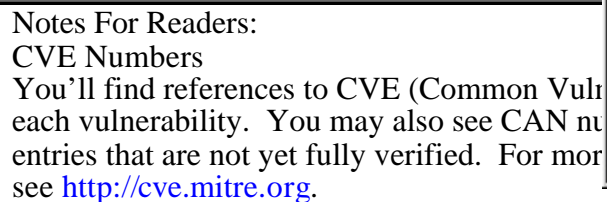
# Where the CVE List comes from





# Outline

- 0 **Background and Motivation**
- 0 **Finding Out About Vulnerabilities**
- 0 **The Problem and a Solution - CVE**
- 0 **CVE Compatibility**
- 0 **The CVE Process**
-  **Summary**





# Policy on the Use of CVE and CVE-Compatible products

## *Protecting the Homeland*

*Report of the  
Defense Science Board Task Force*

*on*

**DEFENSIVE INFORMATION OPERATIONS**  
**2000 Summer Study**  
**Volume II**



March 2001

Office of the Undersecretary of Defense  
For Acquisition, Technology, and Logistics  
Washington, D.C. 20301-3140

**Furthermore, preference should be given to products that are Compatible with the Common Vulnerabilities and Exposures (CVE) list.**

DoD-wide GIG IA tested. The information from GIG opens the lessons learned through the testbed, and if successful in defense testbed avoids the costs and

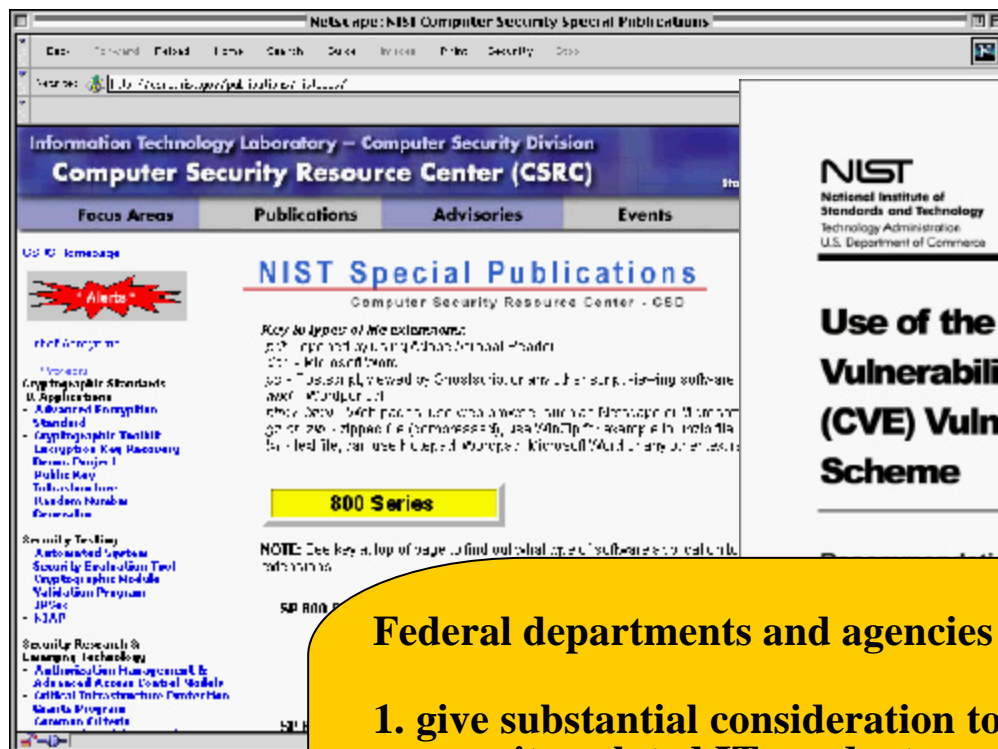
identify quality suppliers of GIG. It is imperative that the information assurance often be bought with service variety of service aspects. For (1) communication speed, 2) ens within certain timelines. In the

pliers' conformance with applicable standards. To and certify compliance with a wide range of the information security arena, conformance the auspices of the National Information. The NIAP is a collaboration between (NIST) and the National Security Agency. The commercial products with security features specified in commercial laboratories to evaluate products against the entry Laboratory Accreditation Program (NVLAP). In should be given to products evaluated under the NIAP.

is to gauge their commitment to fixing security-related to numerous organizations that compile information about among them the Computer Emergency Response Team, the SANS Institute, Security Focus, and NTBugtraq. In should be given to suppliers who have a track record of more, preference should be given to products that are vulnerabilities and Exposures (CVE) list. CVE is a list of exposures that aims to provide common names for CVE is to make it easier to share data across separate with a "common enumeration."

ens of commercial technology need to be understood, the e of adding the technology needs to be weighed before ds that the GIG IA testbed be used to address this issue. deal of publicly available information about technology and d use this information as a starting point for developing act benefits and vulnerabilities.

# National Institute of Standards and Technology (NIST): Policy on the Use of CVE and CVE-Compatible products



## Federal departments and agencies should...

1. give substantial consideration to the acquisition and use of security-related IT products and services that are compatible with the CVE naming scheme.
2. periodically monitor their systems for applicable vulnerabilities listed in the CVE naming scheme.
3. use the CVE vulnerability naming scheme in their descriptions and communications of vulnerabilities

# CVE Has Become Part of Product Comparisons...a step down the road of policy...

Vulnerability Scanner Features								
	Axent Technologies NetRecon 3.0 + SU7	BindView HackerShield	eEye Digital Security Retina	Internet Security Systems Internet Scanner	Nessus Security Scanner	Network Associates CyberCop Scanner	SARA	World Wide Digital Security SAINT
Price	Starts at \$1,995	\$19.95 per IP scanned	Starts at \$1,145	Starts at \$2,795	Free	\$32 per node, \$2,252 server	Free	Free (report generator starts at \$100)
Platform	Windows NT	Windows NT	Windows NT	Windows NT Workstation	Unix	Windows NT	Unix	Unix
Built-in automatic signature update feature	● (download from Web)	●	●	●	● (download from Web)	●	○	○
Scans for host vulnerabilities	○	●	●	●	○	●	○	○
CVE cross-references	○	●	○	●	●	○	●	●
Automatic fixing of select vulnerabilities	○	●	●	○	○	●	○	○
Open source	○	○	○	○	●	○	●	●
Command-line automation	○	○	○	●	●	●	●	●
Integrates with a data- management suite	● (Enterprise Security Manager)	○	○	● (ISS SafeSuite)	○	● (Security Management Interface)	○	○
Capable of custom security checks	○	○	○	○	● (NASL)	● (CASL)	●	●
● Yes ○ No								

Network Computing Article "Vulnerability Assessment Scanners" (1/8/2001)

# CVE Enables Detailed Product Comparisons

## NETWORK IDS FEATURES

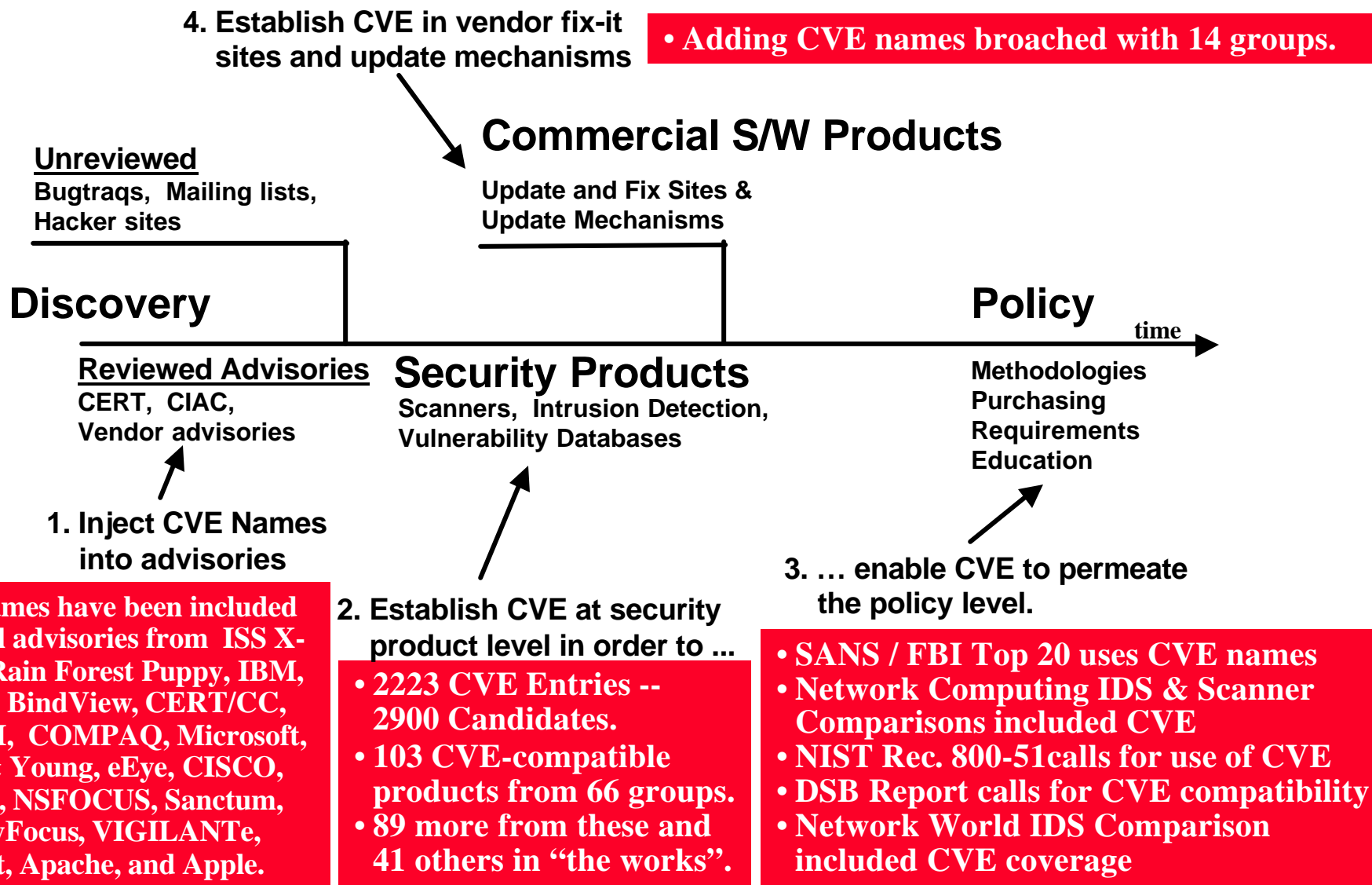
	Cisco Secure IDS 2.5	Computer Associates eTrust	CyberSafe Centrux 2.4	Enterasys Dragon 4.2	Intrusion.com SecureNet Pro 3.2	ISS BlackICE Sentry 2.5	ISS RealSecure 5.5	NFR Security Network Intrusion Detection	Snort 1.7	Symantec NetProver 3.5
Platform	Appliance	Windows NT/ 2000	Windows NT/2000	Appliance, BSD, Linux, Solaris	Appliance, Linux	Windows NT/ 2000	Solaris, Windows NT/ 2000	Appliance	BSD, Linux, Solaris, Windows NT	Windows NT/2000
Held up on the Bruiernet	Y	N	N	Y	Y	Y	Y	Y (on final revision)	Y	N
NIDS/HIDS agents	Y/N	Y/N	Y/Y	Y/Y	Y/N	Y/N	Y/Y	Y/N	Y/N	Y/Y
Integrated HIDS/NIDS management platform	N/A	N/A	Y	Y	N/A	N/A	Y	N/A	N/A	Y
Integrates with file integrity checkers	N	N	Y	Y	N	N	Y	N	N	N
SNMP traps for integration into management platform	N	N	Y	Y	Y	Y	Y	Y	N	Y
Back-end database API	N	N	Y	Y	Y	Y	N	Y	Y (MySQL)	N
Management platform (console)	Windows NT/2000	Windows NT/2000	Windows NT/2000	Unix	Linux	Web	Windows NT/2000	Windows NT/2000	CLI	Windows NT/2000
Remote sensor management	CLI/SPM	Windows NT/2000	Windows NT/2000	CLI/Web	GUI	Windows NT/2000, Web	GUI	Console	CLI	Windows NT/2000
Stealth mode (unbound sniffing NIC)	Y	N	Y	Y	Y	Y	Y	Y	Y	Y
Frag reassembly	Y	N	N	Y	Y	Y	Y	Y	Y	N
TCP stream reassembly	Y	N	N	Y	Y	Y	Y	Y	Y	N
Automatic signature update signatures	N	Y	Y	Y	N	N	Y	Y	Y (if script)	Y
CVE cross-references	N	N	Y	Y	N	Y	N	N	Y (if Whitehat)	Y
Open signature rule sets	N	N	N	N	N	N	N	Y	Y	N
Customizable signatures	Y	Y	N	Y	Y	N	Y	Y	Y	Y
Update frequency	Quarterly and as needed	As needed	Quarterly and as needed	Weekly	Monthly	As needed	Quarterly and mailing list alerts	As needed	Daily releases	N/A

## NETWORK IDS SIGNATURE RESULTS

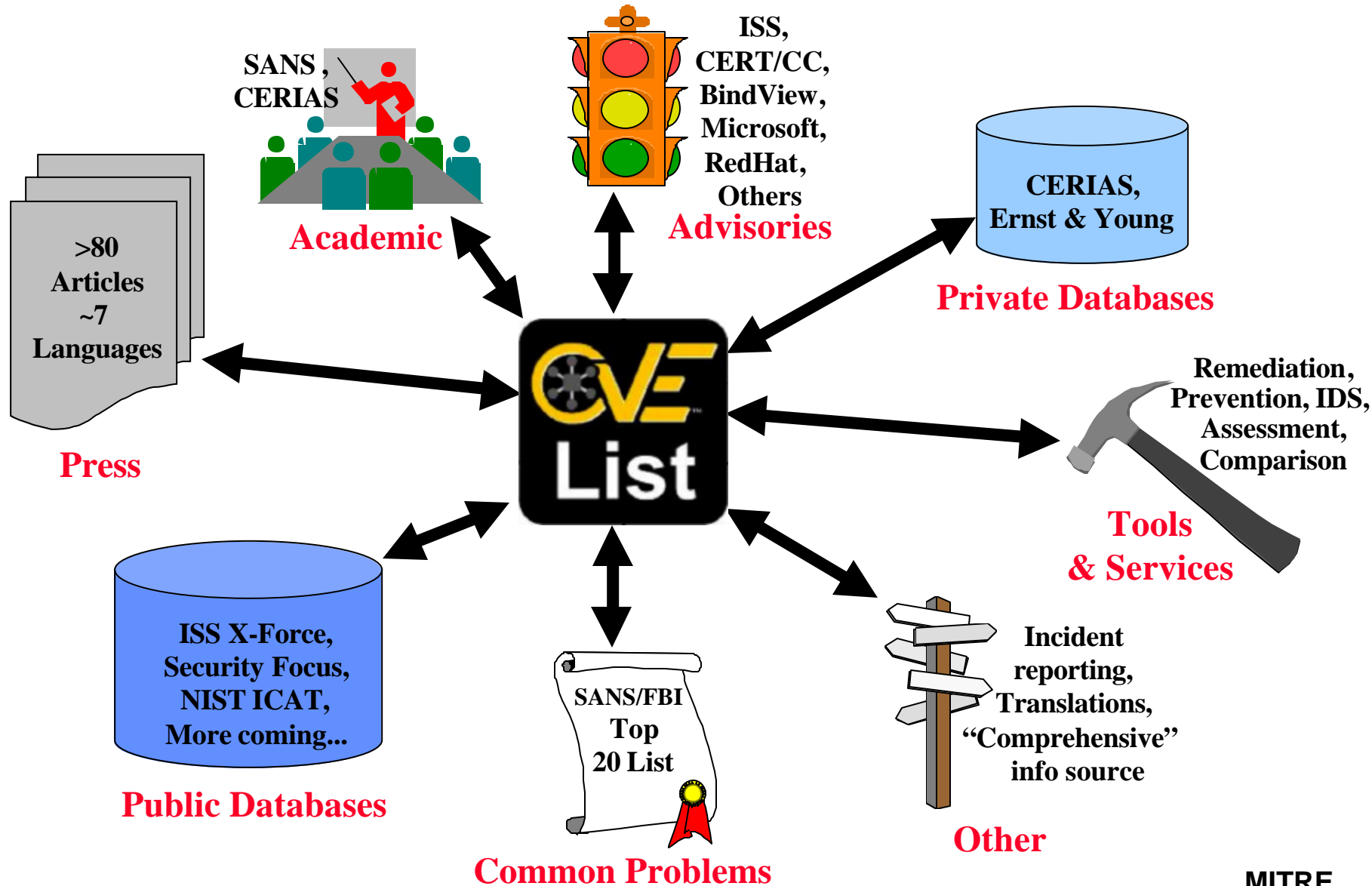
Attack	CVE	No. of packets	Cisco Secure IDS 2.5	Enterasys Dragon 4.2	Intrusion.com SecureNet Pro 3.2	ISS BlackICE Sentry 2.5	ISS RealSecure 5.5	NFR Security Network Intrusion Detection	Snort 1.7	Symantec NetProver 3.5
AMD	CVE-1999-0704	11	Y	Y	N	Y	Y	N	Y	N
RDS	CVE-1999-1011	22	Y	Y	N	Y	Y	Y	Y	Y
WU-FTP	CVE-1999-0368	44	N	Y	N	N	Y	Y	Y	N
SNMP write	CAN-1999-0517	2	N	Y	N	N	Y	Y	N	N
Guest SMB login	CAN-1999-0519	19	N	Y	N	Y	Y	N	Y	N
IMAPD	CVE-1999-0605	8	Y	Y	Y	N	Y	Y	Y	N
PHF	CVE-1999-0667	10	Y	Y	Y	Y	Y	Y	Y	Y
Unicode	CVE-2000-0884	10	Y	Y	N	Y	Y	Y	Y	N
IIS 5 ISAPI	CAN-2001-0241	11	Y	Y	N	N	N	Y	Y	N
Total (out of 9)			6	9	2	5	8	7	8	2
Detest attacks fragmented (Frag-T9)			Y	Y	Y	Y	Y	Y	Y	N

Tables from Network Computing Article "To Catch a THIEF" (8/20/2001)

# The CVE Strategy: Where are we? (as of 24 October 2002)

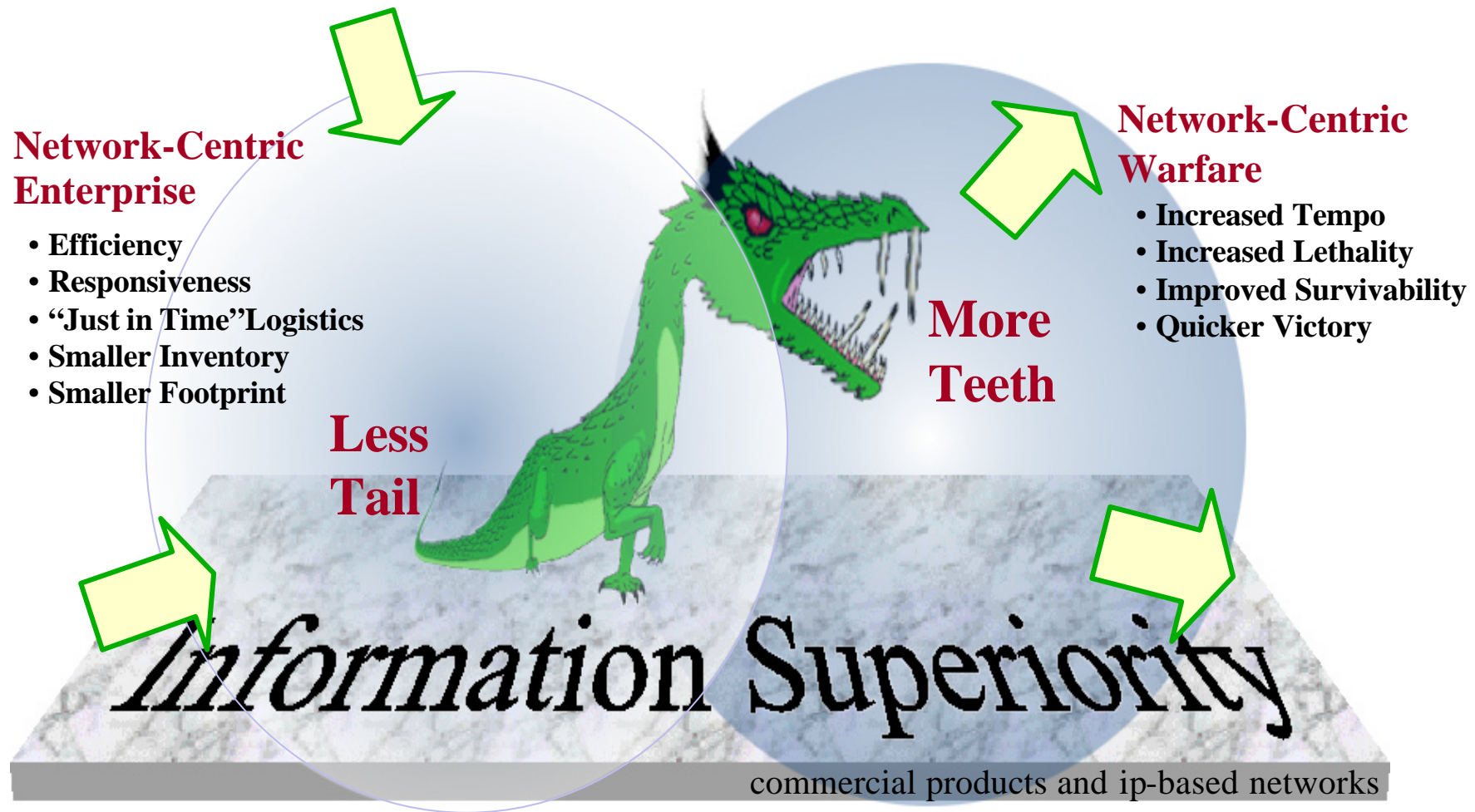


# CVE is the center of many activities and efforts... ...and it's still growing





# CVE is helping make the critical task of effective vulnerability management possible

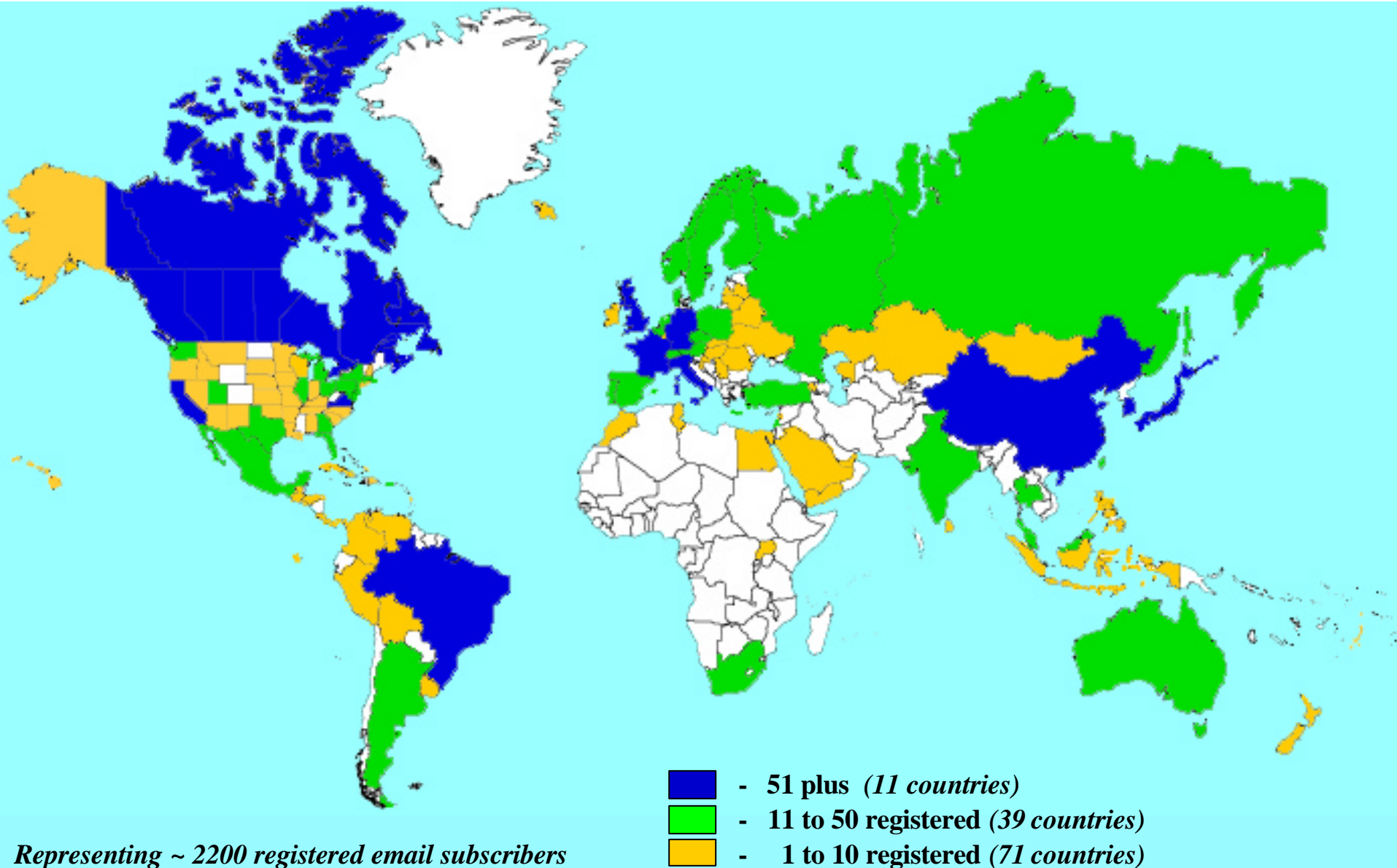


*Commercial-based network-centricism requires management of product vulnerabilities*





# CVE email Lists Have an International Readership





# For More Information



**CVE web site**

**<http://cve.mitre.org>**

